



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/642,318	08/15/2003	Wade Keith Wan	15065US01	2849
23446 7590 11/26/2007 MCANDREWS HELD & MALLOY, LTD 500 WEST MADISON STREET SUITE 3400 CHICAGO, IL 60661			EXAMINER CERVETTI, DAVID GARCIA	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 11/26/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/642,318	WAN ET AL.	
	Examiner	Art Unit	
	David García Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) 23 and 24 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 August 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's arguments filed September 19, 2007, have been fully considered but they are not persuasive.
2. Claims 1-22 are pending and have been examined. Claims 23 and 24 have been withdrawn.

Response to Amendment

3. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.
4. Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.
5. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).
6. Examiner notes the absence of arguments or reply to the rejection of claim 1, as anticipated by Meiyappan (US Patent 6,993,542).

7. Regarding Applicant's argument in reference to claim 1, the feature "a method of generating pseudo-random numbers using a linear feedback shift register in which the correlation between successive pseudo-random numbers is reduced", is taught because the "in which the correlation between successive pseudo-random numbers is reduced" is not a feature of the claim, but a result of the method by "sampling output sequences of said linear feedback shift register with a specified periodicity". This feature, namely "sampling output sequences of said linear feedback shift register with a specified periodicity" is taught in the reference by the cited paragraphs (0096, 0046, abstract, 0026-0027, and 0097), since the numbers are picked at specified clock periods. Therefore, since the method in the reference performs the claimed step, it inherently achieves the same result of "in which the correlation between successive pseudo-random numbers is reduced". **Applicant's arguments are not persuasive.**

8. Regarding Applicant's argument in reference to claim 7, same argument as above applies to the alleged feature of "in which the correlation between successive pseudo-random numbers is reduced".

9. Regarding the step of "periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register" (col. 67 lines 36-col. 68 lines 2), Examiner respectfully submits that "this embodiment switches the connection of the switching circuit 1309 in response to the control signal after a predetermined number of bits are shifted in the LFSR 1302.", clearly anticipating "periodically switching", not after a time

period per se, but after some action takes place. **Applicant's arguments are not persuasive.**

10. Regarding Applicant's argument in reference to claim 11, Thomas clearly teaches the claimed subject matter, as follows, "operating a nonlinear operator on said pseudo-random number and one or more operands" (claim 29, and par. 0213, and 0155, the two taps map to the one or more operands). See also claim 29. **Applicant's arguments are not persuasive.**

11. Regarding Applicant's argument in reference to claim 17, Walmsley clearly teaches "varying the initial value of said hashing function over time by way of a function operating on one or more variables" (0358-0365 and 0942-0943, the use of time varying random number is encrypted for the signature - hash). **Applicant's arguments are not persuasive.**

Claim Rejections - 35 USC § 102

12. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

13. **Claims 1-6, 14-16, and 20-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Gressel et al. 2004/0205095 A1.**

Regarding claim 1, Gressel et al. teaches

- a method of generating pseudo-random numbers using a linear feedback shift register (0044-0046, 0026 and 0098)
- in which the correlation between successive pseudo-random numbers is reduced (0046),

- said method comprising Sampling output sequences of said linear feedback shift register with a specified periodicity (0096, 0046, abstract, 0026-0027, and 0097).

Regarding claim 2, Gressel et al. teaches the method wherein said linear feedback shift register generates said output sequences corresponding to maximal length sequences (0043).

Regarding claim 3, Gressel et al. teaches the method wherein said specified periodicity is equal to the number of bits output by said linear feedback shift register (0175).

Regarding claims 4-6, Gressel et al. teaches the method further comprising periodically switching between iterative outputs generated by two or more linear feedback shift registers (0263-0264, 0281-0282).

Regarding claims 14-16, Gressel et al. teaches the method further comprising operating a nonlinear operator on said pseudo-random number and one or more operands (0217 and 0239).

Regarding claims 20-22, Gressel et al. teaches the method further comprising: receiving said pseudo-random number generated from said linear feedback shift register (0148, 0156; and varying the initial value of said hashing function over time by way of a function operating on one or more variables (0183, 0197, 0372, and 0455).

14. Claims 7-10 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Furuta et al. 5327522.

Regarding claim 7, Furuta et al. teaches

- a method of generating pseudo-random numbers using linear feedback shift registers (col. 44 lines 55-68)
- in which the correlation between successive pseudo-random numbers is reduced (col. 67 lines 36-col. 68 lines 2);
- said method comprising periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register (col. 67 lines 36-col. 68 lines 2).

Regarding claim 8, Furuta et al. discloses the method wherein said linear feedback shift registers comprise linear shift registers capable of generating maximal length sequences (claim 18).

Regarding claims 9 and 10, Furuta et al. teaches the method wherein said pseudo-random numbers are generated with period equal to the sum of each of the individual linear feedback shift register periods (col. 47 lines 47-col. 48 lines 15).

Regarding claim 19, Furuta et al. teaches the method wherein said one or more variables comprises the configuration of feedback taps associated with said linear feedback shift register (Col. 44 lines 55-col. 45 lines 32).

15. Claims 11-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Thomas et al. 2003/0072059 A1.

Regarding claim 11, Thomas et al. discloses

a method of encrypting a pseudo-random number (claim 3)

generated by a linear feedback shift register (par. 0146 and claim 35)

comprising operating a nonlinear operator on said pseudo-random number and one or more operands (claim 29, and par. 0213, and 0155).

Regarding claim 12, Thomas et al. teaches the method wherein said nonlinear operator comprises an XOR function (0146, 0132).

Regarding claim 13, Thomas et al. teaches the method wherein said one or more operands comprises one operand comprising a unique bit sequence corresponding to the LFSR currently used to generate said pseudo-random number (par. 0125-0127, 0155, 0133, and claim 29).

16. Claim 17 is rejected under 35 U.S.C. 102(e) as being anticipated by Walmsley 20050066168 A1.

Regarding claim 17, Walmsley discloses a method of further encrypting a pseudo-random number (par. 0338, 0344, and 0358) generated from a linear feedback shift register (fig. 9) by using a hashing function (0771, and 0774-0775) comprising:~ receiving said pseudo-random number generated from said linear feedback shift register (0358-0365 and 0942-0934); and varying the initial value of said hashing function over time by way of a function operating on one or more variables (0358-0365 and 0942-0934).

17. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Meiyappan USPN 6993542 B1.

Regarding claim 1, Meiyappan discloses a method of generating pseudo-random numbers (col. 1 lines 65-col. 2 lines 2 and col. 1 lines 19-24) using a linear feedback shift register (fig. 1 element 112) in which the correlation between successive

pseudo-random numbers is reduced (col. 1 lines 19-24 and abstract), said method comprising sampling output sequences of said linear feedback shift register with a specified periodicity (col. 3 lines 14-32 and fig. 2 element 206).

Claim Rejections - 35 USC § 103

18. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

19. **Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Furuta et al. 5327522 in view of Gressel et al. 2004/0205095 A1.**

Regarding claim 18, Furuta et al. teaches the method further comprising: receiving said pseudo-random number generated from said linear feedback shift register (col. 44 lines 55-68); Furuta et al. fails to varying the initial value of said hashing function over time by way of a function operating on one or more variables.

However Gressel et al. discloses receiving said pseudo-random number generated from said linear feedback shift register (0148, 0156); and varying the initial value of said hashing function over time by way of a function operating on one or more variables (0183, 0197, 0372, and 0455).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings because they are analogous in LFSR random number generation.

One would have been motivated to incorporate the teachings because it would perform verification of initial value.

Conclusion

20. **Examiner's Note:** Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

21. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David García Cervetti whose telephone number is

Application/Control Number:
10/642,318
Art Unit: 2136

Page 10

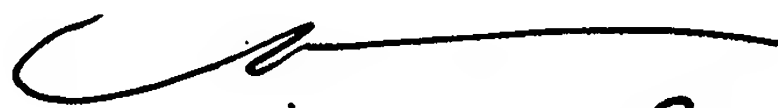
(571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

24. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


11,23,07